On finite metabelian p-groups with two generators

By G. SZEKERES in Adelaide (South Australia)

To Professor L. Rédei for his 60th birthday

1. The structure problem of finite metabelian groups[1]) is an intricate subject about which only some rather isolated and fragmentary results are known.[2]) At present there is no theory in existence, and probably none in sight, which would give a complete account of all existing (finite) metabelian group structures, e. g. along the lines of the well known theory of finite abelian groups. The diversity of metabelian group structures far exceeds that of ordinary abelian groups and compares with the order of diversity of abelian operator groups over commutative rings of operators. The two types of structures have in fact a great deal in common and the study of abelian operator groups seems to be a necessary prerequisite to any comprehensive theory of metabelian groups.

In the present work we shall be concerned with metabelian p-groups with two generating elements where p is a fixed prime number. The abelian operator groups associated with these groups are cyclic (in the sense that they are generated by a single element) and hence structurally identical with polynomial ideals in one or more variables. We shall make use of this relation to determine all metabelian p-groups with two generators which have a commutator subgroup of type $(p, \ldots, p)$; to remove this last mentioned restriction, it would be necessary to know all polynomial ideals in two variables over the integers (or in three variables over a field) for which there is no satisfactory process of enumeration known at the present time.

Denote by $\mathfrak{A}$ the commutator subgroup of the finite metabelian p-group $\mathfrak{G}$. Let $\mathfrak{G}$ be generated by the elements S, T and $\sigma = S\mathfrak{A}$, $\tau = T\mathfrak{A}$ the corresponding cosets modulo $\mathfrak{A}$. Evidently σ, τ are generating elements of the

[1]) We call a group metabelian if its commutator subgroup is abelian and distinct from the identity. All groups considered in this paper are finite.

[2]) A list of metabelian p-groups with known structure has been compiled at the end of the paper.

(abelian) quotient group $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$ and we can assume that they are independent basis elements of $\mathfrak{B}$.[3])

Let $\mathfrak{C}$ denote the ring of rational integers and $\mathfrak{C}[\sigma, \tau]$ the (commutative) ring of polynomials in σ, τ with integer coefficients. $\mathfrak{C}[\sigma, \tau]$ is an operator ring for $\mathfrak{A}$ under the well known rules

$$A^{\varrho} = R^{-1} A R, \quad \varrho = \sigma^{k} \tau^{l}, \quad R = S^{h} T^{l}, \tag{1.01}$$

$$A^{\varrho_1 + \varrho_2} = A^{\varrho_1} A^{\varrho_2}, \quad \varrho_1 \in \mathfrak{C}[\sigma, \tau], \quad \varrho_2 \in \mathfrak{C}[\sigma, \tau]. \tag{1.02}$$

As a $\mathfrak{C}[\sigma, \tau]$-group, $\mathfrak{A}$ is cyclic and is generated by the element

$$A_0 = T^{-1} S^{-1} T S. \tag{1.1}$$

In fact, the equations

$$TS = S T A_0 \tag{1.11}$$

$$A_0^{q(\sigma, \tau)} S = S A_0^{\sigma g(\sigma, \tau)} \tag{1.12}$$

$$A_0^{g(\sigma, \tau)} T = T A_0^{\tau g(\sigma, \tau)}, \quad g(\sigma, \tau) \in \mathfrak{C}[\sigma, \tau] \tag{1.13}$$

allow us to reduce every finite product formed by S and T (hence every element of $\mathfrak{G}$) to the form

$$S^{q} T^{r} A_0^{f(\sigma, \tau)} \tag{1.14}$$

where q, r are non-negative integers and $f(\sigma, \tau)$ has non-negative integer coefficients. But the elements $A_0^{f(\sigma, \tau)}$ form a subgroup $\mathfrak{A}^*$ of $\mathfrak{A}$, viz. the $\mathfrak{C}[\sigma, \tau]$-subgroup generated by A_0, and $\mathfrak{G}/\mathfrak{A}^*$ is abelian, as seen from (1.14), so that $\mathfrak{A}^* \supseteq \mathfrak{A}$, whence $\mathfrak{A}^* = \mathfrak{A}$.

Now the set of annulling polynomials $g(u, v)$ for which $A_0^{g(\sigma, \tau)} = 1$[4]) form an ideal $\mathfrak{J}$ in $\mathfrak{C}[u, v]$ with the property that

$$p^{h} \equiv 0 (\mathfrak{J}), \quad u^{p^m} \equiv 1 (\mathfrak{J}), \quad v^{p^n} \equiv 1 (\mathfrak{J}) \tag{1.2}$$

where p^m, p^n are the respective orders of σ, τ and p^h is the exponent of $\mathfrak{A}$. Conversely, given an ideal $\mathfrak{J}$ which satisfies the conditions (1.2) we can construct all groups $\mathfrak{G}$ which belong to this annulling ideal by taking (1.11)—(1.13) as a set of defining relations for $\mathfrak{G}$ and by specifying S^{p^m}, T^{p^n} as suitable elements of $\mathfrak{A}$. It appears therefore that the first step in the determination of these groups is to enumerate (and possibly characterize by numerical invariants) all ideals in $\mathfrak{C}[u, v]$ which satisfy the conditions (1.2).

---

[3]) $\mathfrak{B}$ is evidently non-cyclic.

[4]) We shall use the symbol 1 to denote the identity element of any algebraic system such as groups, fields or operator rings. There is no danger of confusion as it is always clear from the context which of these identities is represented.

There is an important class of polynomial domains in which a complete enumeration of ideals is known, namely domains of the form $\mathfrak{R}[x]$ where $\mathfrak{R}$ is a (commutative) principal ideal ring. Moreover, a complete characterization of the ideals by numerical (or more general algebraic) invariants is possible if $\mathfrak{R}$ has the further property that each class of associated elements has a uniquely distinguished "normal" representative and each class of residues modulo a given element has a similarly distinguished representative. Such is the case when $\mathfrak{R}=\mathfrak{F}[y]$ where $\mathfrak{F}$ is a field; with each non-zero $f(y)\in\mathfrak{F}[y]$ there is associated a unique $f^*(y)$ with leading coefficient 1 and in each class of residues modulo $f(y)$ there is precisely one $g(y)$ with $\deg g<\deg f$. In the following we shall only be concerned with the case that $\mathfrak{F}$ is the prime field of characteristic p.

A process of enumeration of ideals in $\mathfrak{R}[x]$ was first established by KRONECKER and HENSEL [3] and, independently, by the author [10]; the equivalence of the two systems of enumeration was demonstrated by RÉDEI [6]. The following is an adaptation of the principal result to the case when $\mathfrak{R}[x]=\mathfrak{F}[x,y]$ where $\mathfrak{F}$ is the field of residue classes modulo p.

We first note that every non-zero polynomial of $\mathfrak{F}[y]$,

$$(1.3)\qquad \varphi(y)=a_0+\cdots+a_m y^m,\quad 0\leqq a_i<p\ (i=0,\ldots,m-1),\quad 0<a_m<p$$

can be characterized by a positive integer

$$q=\varphi(p)=a_0+\cdots+a_m p^m;$$

conversely, with each positive integer q there is uniquely associated a polynomial (1.3) of $\mathfrak{F}[y]$. This remark allows us to describe elements of $\mathfrak{F}[y]$ by non-negative integers, and it also introduces a simple ordering of elements of $\mathfrak{F}[y]$ by the rule:

$$(1.31)\qquad \varphi(y)<\psi(y)\quad\text{if and only if}\quad \varphi(p)<\psi(p).$$

To obtain an arbitrary primitive ideal of $\mathfrak{F}[x,y]$ (i. e. an ideal which is not divisible by a non-trivial element of $\mathfrak{F}[x,y]$), we specify

(i) a set of positive integers $d_1,\ldots,d_k$,
(ii) a set of integers $0=s_0<s_1<\cdots<s_k$,
(iii) a set of integers $0\leqq q_{ir}<p^{d_i}$, $\qquad(r=0,\ldots,s_i;\ i=1,\ldots,k)$.

Let $\varphi_{ir}(y)$ be the polynomial (of degree $<d_i$) associated with q_{ir} and define the polynomials $g_0(y)$, $g_i(x,y)$, $(i=1,\ldots,k)$ as follows:

$$(1.41)\qquad g_0(y)=\prod_{i=1}^{k}(y^{d_i}+\varphi_{i,s_i}(y)),$$

$$(1.42)\qquad (y^{d_i}+\varphi_{i,s_i}(y))g_i(x,y)=x^{s_i-s_{i-1}}g_{i-1}(x,y)+\sum_{j=0}^{i-1}\psi_{ij}(x,y)g_j(x,y)$$

where

$$\psi_{ij}(x, y) = \sum_{0 \leqq r < s_{j+1} - s_j} \varphi_{i, s_j + r}(y) x^r \qquad (0 \leqq j < k,\ 1 \leqq i \leqq k). \tag{1.43}$$

Then the ideals

$$\mathfrak{J} = (g_0, g_1, \ldots, g_h) \tag{1.44}$$

which belong to the different systems d_i, s_j, q_{ir} represent exactly once all the primitive ideals of $\mathfrak{P}[x, y]$.[5]

An obvious application of this result is to the structure problem of metabelian p-groups generated by two elements whose commutator subgroup is of the type $(p, \ldots, p)$. For then $h = 1$, $p \equiv 0 (\mathfrak{J})$ in (1.2) and $\mathfrak{J}$ is an ideal in $\mathfrak{P}[u, v]$. The fact that it must also satisfy the second and third condition in (1.2) causes some difficulty which will be resolved in the next section. The actual construction of the groups $\mathfrak{G}$ will be carried out in § 3, and an extension of the result to a further class of metabelian p-groups is discussed in § 4.

2. Since $p = 0$ in $\mathfrak{P}$, the conditions $u^{p^m} \equiv 1, v^{p^m} \equiv 1 (\mathfrak{J})$ are equivalen to $(u-1)^{p^m} \equiv 0, (v-1)^{p^m} \equiv 0 (\mathfrak{J})$. It is convenient to introduce the new variables

$$x = u - 1, \quad y = v - 1$$

corresponding to the operators $\mu = \sigma - 1, \nu = \tau - 1$. Clearly $\mathfrak{A}$ can be regarded as a $\mathfrak{P}[\mu, \nu]$-group and the annulling ideal of A_0 is then an ideal $\mathfrak{J}$ in $\mathfrak{P}[x, y]$ such that

$$x^{p^m} \equiv 0, \quad y^{p^m} \equiv 0 (\mathfrak{J}). \tag{2.0}$$

Since x and y are relatively prime in $\mathfrak{P}[x, y]$, these conditions imply that $\mathfrak{J}$ is a primitive ideal.[6])

The second condition in (2.0) causes no difficulty; it is in fact satisfied if and only if $\varphi_{i, s_i} = 0$ for every i in (1.41). The first condition is much more troublesome; for there seems to be no simple method or algorithm by which to decide from a given system of invariants whether the corresponding $\mathfrak{J}$ contains x^{p^m} or not. Even if such an algorithm existed, it does not seem to be possible to characterize the "good" ideals by means of simple inequalities imposed upon the invariants q_{ir}. Therefore, instead of trying to patch up the system (1.41)—(1.44) to suit conditions (2.0), we shall make a fresh start by assuming right from the beginning that $\mathfrak{J}$ has the property (2.0). Although no explicit use will be made of the Kronecker—Hensel theorem,

---

[5]) [6], p. 200.

[6]) This already follows from the fact that $\mathfrak{P}[x, y]/\mathfrak{J}$ is finite, see RÉDEI [5], § 109.

the work will follow quite closely the method employed for the derivation of (1.41)—(1.44) in [10] and [6].

Suppose that $\mathfrak{J}$ contains the elements x^{p^m}, y^{p^n}. Let l denote the smallest positive integer such that

$$x^l \equiv 0 \ (\mathfrak{J}); \tag{2.01}$$

for $0 \leqq s \leqq l$, denote by c_s the smallest exponent such that

$$y^{c_s} x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}). \tag{2.02}$$

Evidently

$$0 = c_l < c_{l-1} \leqq \cdots \leqq c_0. \tag{2.03}$$

Since (2.0) is assumed, we must have

$$c_0 \leqq p^n, \quad l \leqq p^m. \tag{2.04}$$

In the following we assume that $\mathfrak{J}$ and the corresponding c_s are given.

Lemma 2.1.

implies $\varphi(y) \equiv 0 \ (y^{c_s})$.

$$\varphi(y) x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}), \quad \varphi(y) \in \mathfrak{F}[y] \tag{2.1}$$

We have at any rate $(\varphi(y), y^{c_s}) = y^d$ in $\mathfrak{F}[y]$ where $0 \leqq d \leqq c_s$, hence by (2.02) and (2.1), $y^d x^s \equiv 0 \ (\mathfrak{J}, x^{s+1})$. By the minimal property of c_s, $d \geqq c_s$ hence $d = c_s$, $\varphi(y) \equiv 0 \ (y^{c_s})$.

Lemma 2.2. *If f is an arbitrary polynomial in $\mathfrak{F}[x, y]$ then*

$$f(x, y) \equiv \sum_{s=0}^{l-1} \varphi_s(y) x^s \ (\mathfrak{J}), \quad \varphi_s(y) < y^{c_s} \qquad (s = 0, \ldots, l-1) \tag{2.2}$$

and the coefficients φ_s are uniquely determined by f. The inequality in (2.2) *is in the sense of the ordering* (1.31).

Suppose that we have already proved

$$f \equiv \varphi_0 + \cdots + \varphi_{t-1} x^{t-1} \ (\mathfrak{J}, x^t), \quad \varphi_s < y^{c_s} \quad \text{for} \quad s < t.$$

Write

$$f = \varphi_0 + \cdots + \varphi_{t-1} x^{t-1} + \psi_t x^t \ (\mathfrak{J}, x^{t+1}), \quad \psi_t = \varphi_t + y^{c_t} \varrho_t$$

with $\varphi_t < y^{c_t}$. We have, by (2.02), $\psi_t x^t \equiv \varphi_t x^t \ (\mathfrak{J}, x^{t+1})$ hence $f \equiv \sum_{s=0}^{t} \varphi_s x^s$ $(\mathfrak{J}, x^{t+1})$. The remark that $x^l \equiv 0 \ (\mathfrak{J})$ concludes the proof. Uniqueness follows from Lemma 2.1.

As a corollary we have the result that the elements of $\mathfrak{A}$ can uniquely be written in the form

$$A = A_0^{\sum_{0 \leqq s < l} \varphi_s(\sigma-1)(\tau-1)^s}, \quad \varphi_s(y) < y^{c_s} \qquad (s = 0, \ldots, l-1) \tag{2.21}$$

and the order of $\mathfrak{S}[x, y]/\mathfrak{S}$, hence of $\mathfrak{N}$, is

$$p^h = p^{c_0+\cdots+c_{l-1}}. \tag{2.22}$$

From (2.02) it follows that there exist polynomials $g_s(x, y)$ of the form

$$g_s = y^{c_s}x^s + \sum_{s<t<l} \psi_{st}(y)x^t \equiv 0 \ (\mathfrak{J}) \qquad (s = 0, \ldots, l-1). \tag{2.23}$$

By Lemma 2.1, $\mathfrak{J} = (g_0, \ldots, g_{l-1}, g_l = x^l)$, and we have the problem of enumerating all the essentially different systems (2.23). The chief obstacle in the way of enumeration is that if a system (2.23) is arbitrarily given, it is by no means certain that the c_s which appear in (2.23) are identical with those belonging to $\mathfrak{J} = (g_0, \ldots, g_l)$ in the sense of (2.02). In other words, the c_s in (2.23) do not always possess the required minimum property.

We shall call a system (2.23) *good* if it has the property that

$$\varphi(y)x^s \equiv 0 \quad (g_0, \ldots, g_l, x^{s+1})$$

always implies $\varphi(y) \equiv 0 \ (y^{c_s})$, that is, if Lemma 2.1 is true for $\mathfrak{J} = (g_0, \ldots, g_l)$.

Lemma 2.3. *A system* (2.23) *is good if and only if*

$$xg_s \equiv 0 \ (g_{s+1}, \ldots, g_l) \qquad (s = 0, \ldots, l-1). \tag{2.3}$$

If: Suppose that (2.3) is true for the system $\{g_s\}$. It implies that any expression

$$f_0g_0 + \cdots + f_lg_l, \quad f_s \in \mathfrak{S}[x, y], \qquad (s = 0, \ldots, l)$$

can be written as

$$\sum_{s=0}^{l-1} \varphi_s g_s + f^* g_l, \quad \varphi_s \in \mathfrak{S}[y], \quad f^* \in \mathfrak{S}[x, y].$$

Therefore

$$\varphi(y)x^s \equiv 0 \ (g_s, \ldots, g_l, x^{s+1})$$

for some $s < l$ implies

$$\varphi x^s = \sum_{i=0}^{l-1} \varphi_i g_i + f^* x^{s+1}$$

hence $\varphi_r = 0$ for $r < s$ and $\varphi = \varphi_s y^{c_s}$. By definition, $\{g_s\}$ is a good system.

Only if: We shall prove that if $\{g_s\}$ is good and $x^t f \equiv 0 \ (g_0, \ldots, g_l)$ for some $0 \leqq t \leqq l$ then $x^t f \equiv 0 \ (g_t, \ldots, g_l)$. The statement is trivially true for $t = l$. Suppose it is true for $t+1$ $(t < l)$ and $x^t f \equiv 0 \ (g_0, \ldots, g_l)$. Write $f \equiv \varphi(y) \pmod{x}$ so that $x^t f \equiv x^t \varphi \equiv 0 \ (g_0, \ldots, g_l, x^{t+1})$. This implies, since $\{g_s\}$ is good, that $\varphi = y^{c_t}\psi$, $\psi \in \mathfrak{S}[y]$ and

$$x^t f - \psi g_t + x^{t+1} f^* \equiv 0 \ (g_0, \ldots, g_l)$$

for a suitable $f^* \in \mathfrak{S}[x, y]$. Hence $x^{t+1} f^* \equiv 0 \ (g_0, \ldots, g_l)$ and by the induction hypothesis $x^{t+1} f^* \equiv 0 \ (g_{t+1}, \ldots, g_l)$, $x^t f \equiv 0 \ (g_t, \ldots, g_l)$.

Lemma 2.4. *An ideal $\mathfrak{J}$ which has the property* (2.02) *contains a (necessarily good) set of polynomials* (2.23) *such that*

$$\mathfrak{J} = (g_0, \ldots, g_l \quad - x^l)$$

and

$$xg_s = \sum_{s \leqq t \leqq l} \varphi_{st} g_t, \quad \varphi_{st} \in \mathfrak{S}[y] \tag{2.4}$$

with

$$\varphi_{s,s+1} = y^{c_s - c_{s+1}}, \quad \varphi_{s,t+1} < y^{c_t - c_{t+1}} \quad \text{for} \quad s < t < l. \tag{2.41}$$

Let $s < l$ and suppose that $g_l = x^l$, $g_{l-1}, \ldots, g_{s+1}$ have already been determined so as to satisfy (2.4), (2.41). Let g_s^* be any polynomial $\in \mathfrak{J}$, of degree $< l$ in x and with lowest term $y^{c_s} x^s$. By Lemma 2.3,

$$xg_s^* = \psi_{s+1}(y) g_{s+1} + \cdots + \psi_l(y) g_l$$

hence $\psi_{s+1} = y^{c_s - c_{s+1}} = \varphi_{s,s+1}$. Now suppose that we were able to determine g_s^* so that

$$\psi_{r+1} < y^{c_r - c_{r+1}} \quad \text{for} \quad s < r < t \qquad (t < k).$$

We show the same for $r = t$.

Write $\psi_{r+1} = \varphi_{s,r+1}$ for $r < t$,

$$\psi_{t+1} = \varphi_{s,t+1} + \psi y^{c_t - c_{t+1}}, \quad \varphi_{s,t+1} < y^{c_t - c_{t+1}}.$$

Replace g_s^* by $g_s^{**} = g_s^* - \psi g_t$; then we have

$$xg_s^{**} = xg_s^* - \psi x g_t = \sum_{r=s}^{t-1} \varphi_{s,r+1} g_{r+1} + (\psi_{t+1} - \psi y^{c_t - c_{t+1}}) g_{t+1} +$$

$$+ \sum_{t < r < l} \psi_{r+1}^* g_{r+1} = \sum_{r=s}^{t} \varphi_{s,r+1} g_{r+1} + \sum_{t < r < l} \psi_{r+1}^* g_{r+1}.$$

This proves the Lemma.

To complete the enumeration of the ideals $\mathfrak{J}$ we have to show:

Lemma 2.5. (*a*) *To each system of φ_{st} which satisfy the inequalities* (2.41) *there exists a good system $\{g_s\}$ given by* (2.4), *hence an ideal $\mathfrak{J} = (g_0, \ldots, g_l = x^l)$*; (*b*) *The system φ_{st} is uniquely determined by $\mathfrak{J}$.*

To prove (*a*) it is sufficient to remark that the g_s can obviously be determined recursively from (2.4) and the resulting system is good by Lemma 2.3. In fact the g_s are given explicitly by

$$g_s = \sum_{i=1}^{l-s} \sum_{0 < d_1 < \cdots < d_i = l-s} \varphi_{s,s+d_1} \varphi_{s+d_1,\, s+d_2} \cdots \varphi_{s+d_{i-1},\, i}\, x^{l-i}. \tag{2.51}$$

To prove (b) we have to show that two different systems φ_{st}, φ^*_{st} cannot define the same $\mathfrak{I}$. Suppose that they do belong to the same $\mathfrak{I}$ and suppose also that for some $s<l$, $\varphi_{r,t+1}=\varphi^*_{r,t+1}$ (hence $g_r=g^*_r$) for every $t\geqq r>s$. We have

$$xg_s=\sum_{s<r\leqq l}\varphi_{sr}g_r\,,\quad xg^*_s=\sum_{s<r\leqq l}\varphi^*_{sr}g^*_r=\sum_{s<r\leqq l}\varphi^*_{sr}g_r\,,$$

hence

$$x(g^*_s-g_s)=\sum_{s<r\leqq l}(\varphi^*_{sr}-\varphi_{sr})g_r. \tag{2.52}$$

But $g^*_s\equiv 0\ (g_s,g_{s+1},\ldots,g_k)$ hence $g^*_s=g_s+\sum_{s<r<l}\psi_r g_r$,

$$x(g^*_s-g_s)=\sum_{s<r<l}\psi_r xg_r\,.$$

Suppose that $\psi_r=0$ for $s<r<t$, then

$$x(g^*_s-g_s)=\sum_{t\leqq r<l}\psi_r xg_r=\psi_t\varphi_{t,t+1}g_{t+1}+\sum_{t+1<r\leqq l}\psi^*_r g_r.$$

Comparing with (2.52),

$$\psi_t\varphi_{t,t+1}=\varphi^*_{s,t+1}-\varphi_{s,t+1}<y^{c_t-c_{t+1}}=\varphi_{t,t+1}\,,$$

$$\psi_t=0,\quad (t=s+1,\ldots,l+1),\quad g^*_s=g_s.$$

Lemma 2.5 shows that the g_s given by (2.4), (2.41) form a canonical basis of $\mathfrak{I}$. A more concise form of the basis is obtained if, following RÉDEI, we discard certain unnecessary ones among the g_s. The set $\{c_s\}$ uniquely determines a sequence $0=s_0<s_1<\cdots<s_k=l$ with the property that

$$c_{s_{i+1}}<c_{s_i},\quad c_s=c_{s_i}\quad\text{for}\quad s_i\leqq s<s_{i+1}\qquad (i=0,1,\ldots,k-1).$$

Now from (2.41) we see that $\varphi_{st}=0$ in (2.4) for every t for which $c_{t-1}-c_t=0$ so that

$$xg_s=y^{c_s-c_{s+1}}g_{s+1}+\sum\varphi_{s,s_i}g_{s_i}$$

summed for all i with $s_i>s+1$. Consequently, the g_{s_i} form an ideal basis of $\mathfrak{I}$ and the g_s with $s_i<s<s_{i+1}$ are redundant. If for sake of simplicity we write g_i instead of g_{s_i}, and

$$d_i=c_{s_{i-1}}-c_{s_i}\qquad (i=1,\ldots,k), \tag{2.6}$$

our findings can be summarized as follows:

Definition 2.6. *Given a set of positive integers*

$$d_i>0\qquad (i=1,\ldots,k), \tag{2.61}$$

a set of integers

(2.62) $$0 = s_0 < s_1 < \cdots < s_k = l$$

and a set of integers

(2.63) $$0 \leqq q_{si} < p^{d_i} \qquad (0 < s < s_i,\ 1 \leqq i \leqq k),$$

the ideal

$$\mathfrak{J} = (g_0, \ldots, g_k)$$

of $\mathfrak{F}[x, y]$ *is said to belong to the invariants* (2.61), (2.62), (2.63) *if the* g_i *are obtained from*

(2.64) $$g_k = x^l,$$

(2.65) $$x^{s_{i+1}-s_i} g_i = \sum_{j=i+1}^{k} \psi_{ij}(x, y)\, g_j,$$

(2.66) $$\psi_{ij}(x, y) = \sum_{0 \leqq r < s_{i+1}-s_i} \varphi_{s_{i+1}-r,\,j}(y) x^r \qquad (0 \leqq i < j \leqq k),$$

where

(2.67) $$\varphi_{s_j,\,i} = y^{d_i} \qquad (i = 1, \ldots, k)$$

and $\varphi_{s,i}(y)$ *for* $s < s_i$ *is the polynomial in* $\mathfrak{F}[y]$ *belonging to the integer* q_{si}.

Theorem 1. *To each set of invariants* (2.61), (2.62), (2.63) *there belongs exactly one ideal* $\mathfrak{J}$ *with the property*

(2.71) $$x^l \equiv 0 \ (\mathfrak{J}), \quad y^{c_s} x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}) \qquad (0 \leqq s \leqq l),$$

where

(2.72) $$c_s = \sum_{s_i > s} d_i;$$

c_s *is the smallest integer with property* (2.71).

Conversely, given $\mathfrak{J}$ *with the property* (2.71) *where* c_s *is the smallest such number, and*

(2.73) $$d_i = c_{s_{i-1}} - c_{s_i} \qquad (i = 1, \ldots, k)$$

where

(2.74) $$c_{s_{i+1}} < c_{s_i}, \quad c_s = c_{s_i} \ \text{for} \ s_i \leqq s < s_{i+1} \qquad (i = 0, \ldots, k),$$

there is exactly one system of invariants (2.63) *to which* $\mathfrak{J}$ *belongs.*

It follows from (2.71) that $y^{\sum_{s=0}^{l-1} c_s} \equiv 0 \ (\mathfrak{J})$ so that

(2.75) $$y^{l'} \equiv 0 \ (\mathfrak{J})$$

for some l' with

(2.76) $$l' \leqq \sum_{s=0}^{l-1} c_s.$$

The exact value of l' depends on arithmetic properties of the numbers c_s, q_{st} and cannot be obtained in a straightforward manner. The apparent lack of symmetry in the roles of l and l' is due to the fact that the construction of the canonical basis of Theorem 1 is not symmetrical in x and y.[7]) In fact we can interchange the roles of x and y in the construction of the basis and arrive so at a new set of invariants c_s^*, q_{st}^* which describe exactly the same ideal $\mathfrak{J}$. However, it seems to be rather difficult to formulate an explicit connection between c_s, q_{st} on the one hand, and the „conjugate" invariants c_s^*, q_{st}^* on the other.

3. To construct an arbitrary metabelian group $\mathfrak{G}$ with two generators S, T and commutator subgroup $\mathfrak{A}$ of type $(p, \ldots, p)$, we determine as in § 2 an arbitrary ideal $\mathfrak{J}$ in $\mathfrak{P}[x, y]$ with the property that (2.71) and (2.75) is true for some $l > 0$, $l' > 0$. $\mathfrak{A}$ is defined as a cyclic $P[\sigma, \tau]$-group generated by A_0 and isomorphic to the additive group of the quotient ring $\mathfrak{P}[x, y]/\mathfrak{J}$, through

$$f(x, y) \leftrightarrow A_0^{f(\sigma\ 1, \tau\ 1)}, \quad f(x, y) \in \mathfrak{P}[x, y].$$

Next we specify m, n so that

$$l \leqq p^m, \quad l' \leqq p^n \tag{3.0}$$

where l, l' are the integers in (2.71), (2.75), and define $\mathfrak{G}$ as the group generated by S, T with the relations

$$TS = STA_0 \tag{3.01}$$

$$A_0 S = SA_0^{\sigma} \tag{3.02}$$

$$A_0 T = TA_0^{\tau} \tag{3.03}$$

$$S^{p^m} = H, \quad T^{p^n} = K \tag{3.04}$$

where H, K are suitable elements of $\mathfrak{A}$. Trivially, H and K must be such that

$$H^{\sigma} = H, \quad K^{\tau} = K. \tag{3.05}$$

We also stipulate

$$S^{p^{m-1}} \neq 1, \quad T^{p^{n-1}} \neq 1 \tag{3.06}$$

in case that $H = 1$, $l \leqq p^{m-1}$ or $K = 1$, $l' \leqq p^{n-1}$.

By definition, $\mathfrak{G}$ is an extension of the abelian group $\mathfrak{A}$ of type $(p, \ldots, p)$ by an abelian group $\mathfrak{B}$ of the type (p^m, p^n). A Schreier factorsystem is obtained by taking $S^i T^j$ as the selected representative of $\sigma^i v^j$, $0 \leqq i < p^m$,

---

[7]) This is a defect which is shared by all forms of the canonical basis.

$0 \leqq j < p^n$. The factorsystem

$$C(i_1, j_1; i_2, j_2), \quad 0 \leqq i_\nu < p^m, \quad 0 \leqq j_\nu < p^n, \qquad (\nu = 1, 2)$$

is then defined by

$$S^{i_1} T^{j_1} S^{i_2} T^{j_2} = S^{\{i_1 + i_2\}} T^{\{j_1 + j_2\}} C(i_1, j_1; i_2, j_2), \tag{3.1}$$

$$\{i_1 + i_2\} = i_1 + i_2 - \varepsilon(i_1, i_2) p^m, \quad \{j_1 + j_2\} = j_1 + j_2 - \eta(j_1, j_2) p^n \tag{3.11}$$

where

$$\begin{aligned} \varepsilon(i_1, i_2) &= 0 \quad \text{if} \quad 0 \leqq i_1 + i_2 < p^m \\ &= 1 \quad \text{if} \quad p^m \leqq i_1 + i_2 < 2p^m, \end{aligned} \tag{3.12}$$

$$\begin{aligned} \eta(j_1, j_2) &= 0 \quad \text{if} \quad 0 \leqq j_1 + j_2 < p^n \\ &= 1 \quad \text{if} \quad p^n \leqq j_1 + j_2 < 2p^n. \end{aligned} \tag{3.13}$$

To determine $C(i_1, j_1; i_2, j_2)$ explicitly, we observe first that

$$T^j S^i = S^i T^j A_0^{(1+\sigma+\cdots+\sigma^{i-1})(1+\tau+\cdots+\tau^{j-1})} \qquad (i > 0, \ j > 0). \tag{3.14}$$

(3.14) can be verified by induction with the help of the generating relations (3.01)—(3.03) first for $i = 1$ and $j \geqq 1$ then for fixed $j \geqq 1$ and arbitrary $i \geqq 1$. The formula is also valid for $i = 0$, provided that $1 + \cdots + \sigma^{i-1}$ is interpreted to be 0 for $i = 0$; similarly we agree that $1 + \cdots + \tau^{j-1} = 0$ for $j = 0$.

From (3.14) we obtain immediately

$$S^{i_1} T^{j_1} S^{i_2} T^{j_2} = S^{i_1 + i_2} T^{j_1 + j_2} A_0^{(1+\cdots+\sigma^{i_1-1})(1+\cdots+\tau^{j_1-1})\tau^{j_2}}$$

and hence by an easy computation from (3.05), (3.1), (3.11)

$$C(i_1, j_1; i_2, j_2) = A_0^{(1+\cdots+\sigma^{i_2-1})(1+\cdots+\tau^{j_1-1})\tau^{j_2}} H^{\varepsilon(i_1, i_2)\tau^{j_1+j_2}} K^{\eta(i_1, j_2)}. \tag{3.15}$$

The Schreier conditions to be satisfied are

$$\begin{aligned} &C(i_1, j_1; \{i_2 + i_3\}, \{j_2 + j_3\}) C(i_2, j_2; i_3, j_3) = \\ &= C(\{i_1 + i_2\}, \{j_1 + j_2\}; i_3, j_3) C(i_1, j_1; i_2, j_2)^{\sigma^{i_3}\tau^{j_3}}. \end{aligned} \tag{3.16}$$

If we put here first $i_1 = 0, i_2 = 1, i_3 = p^m - 1, j_1 = 1, \ j_2 = j_3 = 0$ then $i_1 = i_2 = 0, i_3 = 1, \ j_1 = p^n - 1, j_2 = 1, j_3 = 0$, we obtain

$$H^{1-\tau} = A_0^{1+\cdots+\sigma^{p^m-1}}, \quad K^{\sigma-1} = A_0^{1+\cdots+\tau^{p^n-1}},$$

hence with (3.05)

$$H^{\sigma-1} = 1, \quad H^{\tau-1} = A_0^{-(1+\cdots+\sigma^{p^m-1})}, \tag{3.17}$$

$$K^{\sigma-1} = A_0^{1+\cdots+\tau^{p^n-1}}, \quad K^{\tau-1} = 1. \tag{3.18}$$

Conversely one can verify that (3.17), (3.18) are sufficient for all Schreier conditions (3.16) to be satisfied so that (3.17), (3.18) are the only restrictions to which H and K are subjected.

Let us write

$$H = A_0^{h(\sigma-1,\tau-1)}, \quad K = A_0^{h(\sigma-1,\tau-1)}; \tag{3.19}$$

we then have the condition that

$$xh(x,y) \equiv 0, \quad yh(x,y) \equiv -x^{p^m-1} \ (\mathfrak{J}) \tag{3.21}$$

$$xk(x,y) \equiv y^{p^n-1}, \quad yk(x,y) \equiv 0 \ (\mathfrak{J}). \tag{3.22}$$

We want to characterize all polynomials $h(x,y)$, $k(x,y)$ which satisfy these congruences.

Suppose first that

$$l < p^m \tag{3.23}$$

so that $x^{p^m-1} \equiv 0 \ (\mathfrak{J})$ and

$$xh(x,y) \equiv yh(x,y) \equiv 0 \ (\mathfrak{J}) \tag{3.24}$$

is valid instead of (3.21).

Now, a polynomial $h(x,y)$ which satisfies $xh \equiv 0 \ (\mathfrak{J})$ can be written uniquely in the form

$$h \equiv \sum_{s=1}^{l} \varphi_s(y) \frac{1}{x} g_s^* \ (\mathfrak{J}) \qquad (0 \leqq \varphi_s < y^{e_{s-1}-e_s}) \tag{3.25}$$

where the g_s^* are the polynomials g_s of Lemma 2.4. This can be shown by the same argument as used in the proof of Lemmas 2.4 and 2.5. Since $\varphi_s(y) = 0$ if $c_{s-1} - c_s = 0$, we can also write

$$h \equiv \sum_{j=1}^{k} \psi_i(y) \frac{1}{x} g_i \ (\mathfrak{J}) \qquad (0 \leqq \psi_i (= \varphi_{s_i}) < y^{d_i}) \tag{3.26}$$

where $g_i = g_{s_i}^*$. The second condition in (3.24) can now be expressed as

$$\sum_{j=1}^{k} y\psi_j(y) \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}). \tag{3.27}$$

Lemma 3.3. *Let $\varphi_{sj}(y)$ be as in Theorem* 1,

$$a_{ij} = \varphi_{s_i,j}(0) \qquad (1 \leqq i \leqq j \leqq k). \tag{3.3}$$

Let $(\xi_1, \ldots, \xi_k)$ be a solution vector over $\mathfrak{F}$ of the linear homogeneous system

$$\sum_{i=1}^{j} \xi_i a_{ij} = 0 \qquad (j = 1, \ldots, k), \tag{3.31}$$

and set

$$y\psi_j(y) = -\sum_{i=1}^{j} \xi_i \varphi_{s_i,j}(y) \qquad (j = 1, \ldots, k); \tag{3.32}$$

then the congruence (3.27) *holds.*

Conversely, every set of $\psi_j \in \mathfrak{S}[y]$, $(j = 1, \ldots, k)$ *for which* (3.27) *is true can be written uniquely in the form* (3.32) *where* $(\xi_1, \ldots, \xi_k)$ *is a solution vector of* (3.31).

It follows from Lemma 3.3 that an $h(x, y)$ which satisfies (3.24) can be characterized completely by a solution vector $\xi = (\xi_1, \ldots, \xi_k)$ of (3.31). Note that the $\psi_j(y)$ defined by (3.32) are polynomials, because of (3.31). Note also that

$$a_{ii} = 0 \qquad (i = 1, \ldots, k) \tag{3.33}$$

from (3.36) below, so that the rank of the system (3.31) is always less than k. In particular, $\xi_i = 0$ for $1 \leqq i < k$, $\xi_k \neq 0$ is a non-zero solution of (3.31). The corresponding $h(x, y)$ is given by

$$h(x, y) = \xi_k y^{d_k - 1} x^{s_k - 1}. \tag{3.34}$$

The proof of the Lemma is based on the formula

$$\sum_{j=i}^{k} \varphi_{s_i,j}(y) \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}) \qquad (i = 1, \ldots, k) \tag{3.35}$$

with

$$\varphi_{s_i,i} = y^{d_i}, \quad 0 \leqq \varphi_{s_i,j}(y) < y^{d_j} \qquad (i < j \leqq k). \tag{3.36}$$

The formula follows directly from (2.65), (2.66) and the fact that $g_i \equiv 0$ $(\mathfrak{J})$.

Suppose now that the ξ_i are a solution of (3.31) and ψ_j is given by (3.32). Substitution into the left hand member of (3.27) gives

$$\sum_{j=1}^{k} y\psi_j \frac{1}{x} g_j = \sum_{j=1}^{k} \sum_{i=1}^{j} \xi_i \varphi_{s_i,j} \frac{1}{x} g_j = \sum_{i=1}^{k} \xi_i \sum_{j=i}^{k} \varphi_{s_i,j} \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J})$$

by (3.35), as required.

Conversely, suppose that the ψ_j satisfy (3.27); then

$$\sum_{j=1}^{q} y\psi_j \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}, x^{s_q}), \qquad (q = 1, \ldots, k) \tag{3.37}$$

and we show that (3.37) holds for $q \leqq r$ $(r \leqq k$ given) only if $\psi_1, \ldots, \psi_r$ are of the form (3.32) where ξ_j $(j = 1, , \ldots, r)$ is a solution of (3.31) for $j = 1, \ldots, r$.

Suppose that the statement is true for $r-1$ (in the case of $r=1$ the assumption is empty), i. e. ψ_j for $j<r$ is of the form (3.32). Substitution into the left hand member of (3.37) gives, by (3.35) and the definition of g_j,

$$y\psi_r \frac{1}{x} g_r + \sum_{j=1}^{r-1} y\psi_j \frac{1}{x} g_j = y\psi_r \frac{1}{x} g_r + \sum_{j=1}^{r-1} \sum_{i=1}^{j} \xi_i \varphi_{s_i,j} \frac{1}{x} g_j =$$

$$= y\psi_r \frac{1}{x} g_r + \sum_{i=1}^{r-1} \xi_i \sum_{j=i}^{r-1} \varphi_{s_i,j} \frac{1}{x} g_j$$

$$\equiv y\psi_r \frac{1}{x} g_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \frac{1}{x} g_r \quad (\mathfrak{J}, x^{s_r})$$

$$\equiv \left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} x^{s_r-1} \quad (\mathfrak{J}, x^{s_r}),$$

hence by (3.37),

$$\left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} x^{s_r-1} \equiv 0 \quad (\mathfrak{J}, x^{s_r}).$$

This can only hold, by definition of the s_r and c_s, if

$$\left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} \equiv 0 \quad (y^{c_{s_r-1}}),$$

$$y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \equiv 0 \quad (y^{d_r}),$$

i. e. if

$$y\psi_r = \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} + \xi_r y^{d_r}$$

for some $\xi_r \in \mathfrak{S}$ which is uniquely determined by ψ_r (since $\varphi_{s_i,r} < y^{d_r}$, $(i=1,\ldots,r-1)$, and $\psi_r < y^{d_r}$). Hence

$$y\psi_r = \sum_{i=1}^{r} \xi_i \varphi_{s_i,r}$$

and the right hand side must be divisible by y, implying

$$\sum_{i=1}^{r} \xi_i a_{ir} = 0.$$

This proves the statement and the Lemma.

If $l=p^m$ then we have (3.21) instead of (3.24) and

$$\sum_{i=1}^{k} y\psi_i \frac{1}{x} g_i + x^{l-1} \equiv 0 \quad (\mathfrak{J}) \tag{3.38}$$

instead of (3.27). A trivial modification of the proof of Lemma 3.3 shows that the solutions of (3.38) are given by

$$y\psi_j(y) = \sum_{i=1}^{j} \xi_i \varphi_{s_i,j}(y) - \delta_{jk} \qquad (j = 1, \ldots, k) \tag{3.39}$$

where $(\xi_1, \ldots, \xi_k)$ is a solution of

$$\sum_{i=1}^{j} \xi_i a_{ij} = \delta_{jk} \qquad (j = 1, \ldots, k) \tag{3.40}$$

($\delta_{jk} = 1$ for $j = k$, 0 for $j \neq k$). Hence not all systems of invariants are admissible but only those for which (3.40) has a solution vector, that is, for which the vector $(a_{1k}, \ldots, a_{kk})$ is linearly independent of the $(a_{1j}, \ldots, a_{jj}, 0, \ldots, 0)$ $(j = 1, \ldots, k-1)$.

To characterize $k(x, y)$ in (3.22) we can use the same method as for $h(x, y)$, provided that $l' < p^n$. The equations to be satisfied are then $xk(x, y) \equiv \equiv yk(x, y) \equiv 0$ $(\mathfrak{S})$ and the $k(x, y)$ are obtained from Lemma 3.3. If $l' = p^n$, however, the method cannot be used directly and it seems best to make use of the conjugate invariants c_s^*, s_i^*, q_{si}^*, obtained by interchanging the roles of x and y in Theorem 1. If $\varphi_{si}^*(y)$ are the corresponding polynomials and $a_{ij}^* = \varphi_{s_i^*,j}^*(0)$ then $k(x, y)$ is given by

$$k(x, y) = \sum_{j=1}^{k^*} \psi_j^*(y) \frac{1}{x} g_j^*, \tag{3.26*}$$

$$y\psi_j^*(y) = \sum_{i=1}^{j} \xi_i^* \varphi_{s_i^*,j}^*(y) + \delta_{jk^*} \qquad (j = 1, \ldots, k^*) \tag{3.39*}$$

where $\xi^* = (\xi_1^*, \ldots, \xi_{k^*}^*)$ is a solution vector of

$$\sum_{i=1}^{j} \xi_i^* a_{ij}^* = -\delta_{jk^*} \qquad (j = 1, \ldots, k^*). \tag{3.40*}$$

For the sake of uniformity it is perhaps better to use the conjugate invariants even if $l' < p^n$; we then have

$$y\psi_j^*(y) = \sum_{i=1}^{j} \xi_i^* \varphi_{s_i^*,j}^*(y) \qquad (j = 1, \ldots, k^*), \tag{3.32*}$$

$$\sum_{i=1}^{j} \xi_i^* a_{ij}^* = 0 \tag{3.31*}$$

with $k(x, y)$ given by (3.26*).

Theorem 2. *A metabelian p-group with two generators S, T and commutator subgroup of type* $(p, \ldots, p)$ *is completely specified by* (i) *a set of integers* d_i, s_i, q_{si} *subject to the conditions* (2.61), (2.62) *and* (2.63) *with*

$l > 1$, (ii) *integers* m, n *subject to* (3.0), (iii) *solution vectors* ξ, ξ^s *of* (3.31), (3.31^s) *if there is strict inequality in* (3.0) *or of* (3.40), (3.40*) *if the equality sign is valid in* (3.0).

The construction of the group $\mathfrak{G}$ *is carried out in the following steps:*

1. *Construct a cyclic* $\mathfrak{F}[\sigma-1, \tau-1]$*-group* $\mathfrak{A} = \{A_0\}$ *with annulling ideal* $\mathfrak{I}$ *where* $\mathfrak{I}$ *is the ideal belonging to the invariants* (i) *according to Definition* 2.6.

2. *Define* $H \in \mathfrak{A}$, $K \in \mathfrak{A}$ *as in* (3.19), *with* $h(x, y), k(x, y)$ *given by* (3.26), (3.26*) *where* ξ, ξ^s *are the invariants* (iii).

3. *Define* $\mathfrak{G}$ *by the generating relations* (3.01)—(3.04) *where* m, n *are the invariants* (ii).

We have called the system of numbers (i), (ii), (iii) of Theorem 2 invariants of $\mathfrak{G}$; in fact, to each such system there belongs precisely one metabelian $\mathfrak{G}$ and each $\mathfrak{G}$ with the specified properties can be obtained in this manner. Nevertheless the system (i), (ii), (iii) is not a true system of invariants; for $\mathfrak{G}$ can usually be obtained from several different such systems. There are two ways in which one can change the invariants of a given $\mathfrak{G}$.

First, one can select new representatives

$$S_1 = SB, \quad T_1 = TC, \qquad B \in \mathfrak{A}, \quad C \in \mathfrak{A} \tag{3.41}$$

of the cosets σ, τ of $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$. Secondly one can replace σ, τ by new basis elements of $\mathfrak{B}$.

The first of these changes implies a replacement of $A_0 = T^{-1}S^{-1}TS$ by

$$A_1 = T_1^{-1}S_1^{-1}T_1S_1 = T^{-1}S^{-1}TSB^{1-\tau}C^{\sigma-1} = A_0B^{-(\tau-1)}C^{\sigma-1}$$

and a replacement of $H = S^{p^m}$, $K = T^{p^n}$ by

$$H_1 = S_1^{p^m} = S^{p^m}B^{1+\sigma+\cdots+\sigma^{p^m-1}} = HB^{(\sigma-1)p^m-1}, \quad K_1 = T_1^{p^n} = KC^{(\tau-1)p^{n-1}}.$$

These changes do not affect the ideal $\mathfrak{I}$, hence s_i, d_i, q_{si}, in any way, also not m and n. Furthermore

$$A^{h(\sigma-1,\tau-1)} = A^{h(\sigma-1,\tau-1)}B^{-(\tau-1)h(\sigma-1,\tau-1)}C^{(\sigma-1)h(\sigma-1,\tau-1)} = HB^{(\sigma-1)p^m-1} = H_1$$

by (3.17) and (3.19), and similarly

$$A_1^{k(\sigma-1,\tau-1)} = K_1.$$

Hence, $h(x, y), k(x, y)$ remain unchanged and the system of invariants of $\mathfrak{G}$ is completely independent of the particular representatives (3.41) of the cosets σ, τ.

Not quite so simple is the case with the second type of change, viz. transition to a new basis in $\mathfrak{B}$. Even the simplest of these transformations, namely interchange of the two basis elements, is non-trivial as it causes the invariants to be replaced by their conjugate system. Other transformations of the basis elements may change the ideal $\mathfrak{I}$ itself. The enumeration of the groups $\mathfrak{G}$ in Theorem 2. cannot be regarded as wholly satisfactory until the problem of selection of a well-defined representative among equivalent systems of invariants is solved.[8])

4. There is a further class of metabelian p-groups with two generators which can be determined by the previous method, namely the ones which contain an abelian normal subgroup $\mathfrak{A}$ such that $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$ is cyclic. We shall indicate briefly the necessary steps. It can be assumed that $\mathfrak{A}$ is a smallest subgroup with the above property. Let S, T be generators of $\mathfrak{G}$. At least one of them, say T, is a representative of a generating coset $\tau = T\mathfrak{A}$ of $\mathfrak{B}$. Then $S = T^q A_0$, $A_0 \in \mathfrak{A}$, hence T and A_0 generate S, therefore they generate $\mathfrak{G}$.

Take a fixed $A_0 \in \mathfrak{A}$ such that T and A_0 generate $\mathfrak{G}$. $\mathfrak{A}$ is now a $\mathcal{C}[\tau]$-group and as such it is generated by A_0. For, if $\mathfrak{A}^*$ is the subgroup of elements $A_0^{f(\tau)}$ then clearly $\mathfrak{A}^* \subseteq \mathfrak{A}$ and $\mathfrak{G}/\mathfrak{A}^*$ is cyclic, hence by the assumption on $\mathfrak{A}$, $\mathfrak{A}^* = \mathfrak{A}$.

The annulling ideal of A_0 is an ideal $\mathfrak{j}$ in $\mathcal{C}[x]$ under the correspondence $\tau - 1 \leftrightarrow x$ with the properties

$$p^h \equiv 0 \ (\mathfrak{j}) \tag{4.11}$$

$$x^l \equiv 0 \ (\mathfrak{j}) \tag{4.12}$$

for suitable positive integers h, l. The first is trivial (p^h is simply the exponent of $\mathfrak{A}$), the second follows from

$$\tau^{p^n} = 1 \tag{4.13}$$

where p^n is the order of $\mathfrak{B}$. For by (4.13), $(\tau-1)^{p^n} \equiv 0 \ (p)$, $(\tau-1)^{hp^n} \equiv 0 \ (p^h)$ hence by (4.11), $(\tau-1)^{hp^n} \equiv 0 \ (\mathfrak{j})$.

If it were not for the condition (4.12), the enumeration of the ideals $\mathfrak{j}$ would be a matter of straightforward application of the Kronecker—Hensel theorem. Because of (4.12) we must proceed as in § 2.

Definition 4.2. *Given a set of positive integers*

$$d_i > 0 \qquad (i = 1, \ldots, k), \tag{4.21}$$

a set of integers

$$0 = s_0 < s_1 < \cdots < s_k = l \tag{4.22}$$

[8]) The problem is analogous to (though not identical with) the determination of all non-isomorphic cyclic rings, as discussed by Rédei in [5], § 109.

and a set of integers

$$0 \leqq q_{si} < p^{d_i} \qquad (0 < s < s_i, \quad 1 \leqq i \leqq k) \tag{4.23}$$

the ideal

$$\mathfrak{J} = (g_0, \ldots, g_k)$$

is said to belong to the invariants (4.21), (4.22), (4.23)[9]) *if the* g_i *are obtained from*

$$g_k = x^l \tag{4.24}$$

$$x^{s_{i+1}-s_i} g_i = \sum_{j=i+1}^{k} \psi_{ij}(x) g_j \tag{4.25}$$

where

$$\psi_{ij}(x) = \sum_{0 \leqq r < s_{i+1}-s_i} q_{s_{i+1}-r} x^r \qquad (0 \leqq i < j \leqq k) \tag{4.26}$$

with

$$q_{s_i, i} = p^{d_i} \qquad (i = 1, \ldots, k). \tag{4.27}$$

By trivial modifications of the argument in § 2 one obtains

Theorem 3. *To each set of invariants* (4.21), (4.22), (4.23) *there belongs exactly one ideal* $\mathfrak{J}$ *with the property*

$$x^l \equiv 0 \ (\mathfrak{J}), \quad p^{e_s} x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}) \qquad (0 \leqq s < l) \tag{4.31}$$

where

$$c_s = \sum_{s_i > s} d_i. \tag{4.32}$$

c_s *is the smallest number with property* (4.31).

Conversely, given $\mathfrak{J}$ *with the property* (4.31) *where* c_s *is the smallest such number, and*

$$d_i = c_{s_{i-1}} - c_{s_i} \qquad (i = 1, \ldots, k) \tag{4.33}$$

where

$$c_{s_i+1} < c_{s_i}, \quad c_s = c_{s_i} \ \text{for} \ s_i \leqq s < s_{i+1} \qquad (i = 0, \ldots, k), \tag{4.34}$$

there is exactly one system of invariants (4.23) *to which* $\mathfrak{J}$ *belongs.*

From (4.31) we conclude that there is a smallest h and m such that

$$p^h \equiv 0 \ (\mathfrak{J}), \quad (x+1)^{p^m} \equiv 1 \ (\mathfrak{J}). \tag{4.35}$$

The exact values of h and m depend on arithmetic properties of c_s, q_{si} and

[9]) $\mathfrak{J}$ is an ideal in $\mathfrak{C}[x]$ so that there is no danger of confusion with Definition 2.6.

must be determined in each individual case; the estimates

$$h \leqq \sum_{s=0}^{l-1} c_s, \quad p^m < l p^h \tag{4.36}$$

are trivial. The order of $\mathcal{C}[x]/\mathfrak{J}$ is p^r, $r = \sum_{s=0}^{l-1} c_s$.

To construct an arbitrary metabelian group $\mathfrak{S}$ with the required properties we start from an ideal $\mathfrak{J}$ with $l > 1$, as obtained in Theorem 3, and define a cyclic $\mathcal{C}[\tau]$-group $\mathfrak{A}$ generated by A_0 and isomorphic to the additive group of the quotient ring $\mathcal{C}[x]/\mathfrak{J}$ through

$$f(x) \longleftrightarrow A_0^{f(\tau-1)}, \quad f(x) \in \mathcal{C}[x].$$

We then determine n so that

$$n \geqq m \tag{4.4}$$

where m is the integer in (4.35), and define $\mathfrak{S}$ by the relations

$$A_0 T = T A_0^{\tau} \tag{4.41}$$

$$T^{p^n} = K = A_0^{k(\mu)} \quad \mu = \tau - 1, \tag{4.42}$$

where $k(x)$ is a suitable polynomial of $\mathcal{C}[x]$. By taking T^j $(0 \leqq j < p^n)$ as the selected representative of τ^j, the Schreier conditions are satisfied if

$$K^{\tau} = K \tag{4.43}$$

i. e. if

$$x k(x) \equiv 0 \ (\mathfrak{J}). \tag{4.44}$$

A polynomial which satisfies (4.44) can be written uniquely in the form

$$k(x) = \sum_{i=1}^{k} b_i \frac{1}{x} g_i(x), \quad 0 \leqq b_i < p^{d_i} \qquad (i = 1, \ldots, k) \tag{4.45}$$

where the $d_i, g_i(x)$ are from Theorem 3. As there are no further conditions on $k(x)$, K is completely characterized by a set of numbers b_i $(i = 1, \ldots, k)$ to be chosen freely in the range $0 \leqq b_i < p^{d_i}$.

A simple calculation shows that for a fixed set of c_s, the number of ways in which one can assign values to the invariants q_{s_i} and b_i is p^r, $r = \sum_{s=0}^{l-1} c_s$, which is just the order of $\mathfrak{A}$. Hence the total number of distinct $\mathcal{C}[\tau]$-groups of order p^r, to which an element K with the property (4.43) has been assigned, is

$$p^r N(r), \tag{4.46}$$

where $N(r)$ is the number of unrestricted partitions of r. For comparison note that $N(r)$ is the number of distinct (ordinary) abelian groups of order p^r.

Turning now to the question of equivalence of the various systems of invariants b_i, d_i, q_{si}, the following changes must be considered:

(a) Replace T by a new representative $T_1 = TB$, $B \in \mathfrak{A}$ of the coset τ.

(b) Replace A_0 by a new generator $A_1 = A_0^{\varphi(t)}$ of $\mathfrak{A}$.

(c) Replace τ by a new generator $\tau_1 = \tau^j$, $(j, p) = 1$ of $\mathfrak{B}$.

(d) Replace $\mathfrak{A}$ by another minimal abelian normal subgroup $\mathfrak{A}^*$ with cyclic quotient group $\mathfrak{B}^* = \mathfrak{G}/\mathfrak{A}^*$.

(a) and (b) affect the numbers b_i, but not the other invariants. They cause $k(x)$ to be replaced by

$$ak(x) + b\pi_n(x) \tag{4.51}$$

modulo $\mathfrak{J}$ where

$$\pi_n(x) = \sum_{i=1}^{p^n} \binom{p^n}{i} x^{i-1} \tag{4.52}$$

and a, b are integers. Note that $x\pi_n(x) = x^{p^n} - 1 \equiv 0$ $(\mathfrak{J})$, so that (4.51) is a legitimate transformation.

A replacement of τ by $\tau_1 = \tau^j$, $(j, p) = 1$ induces a transformation of $\mathfrak{J}$ into the ideal $\mathfrak{J}^*$ formed by all polynomials which have the form $f^*(x) = f((x+1)^i - 1)$ where $f(x) \in \mathfrak{J}$ and $ij \equiv 1 \pmod{p^n}$. Neither of the transformations (a), (b), (c) can be expressed in the form of a simple explicit transformation law of the b_i, q_{si}.

The existence of a second subgroup $\mathfrak{A}^*$ as envisaged under (d) is rather exceptional. It requires T to commute with each element of the commutator subgroup K, which is so if and only if

$$x^2 \equiv 0 \ (\mathfrak{J}), \tag{4.53}$$

i. e. $l = 2$ in (4.22). $\mathfrak{A}^*$ is then the subgroup generated by T and K.

There are two classes of invariants compatible with $l = 2$:

$$k = 1, \quad s_0 = 0, \quad s_1 = 2 \tag{4.54}$$

$$k = 2, \quad s_0 = 0, \quad s_1 = 1, \quad s_2 = 2. \tag{4.55}$$

In the first case we have (with $d = d_1$, $q = q_{11}$, $b = b_1$)

$$g_0(x) = p^d + qx, \quad g_1(x) = x^2, \quad k(x) = bx,$$
$$0 \leqq q < p^d, \quad 0 \leqq b < p^d, \quad n \geqq m = d.$$

It is easy to verify that this system is equivalent to

$$g_0(x) = p^d + p^{a_1}x, \quad g_1(x) = x^2 \tag{4.56}$$

$$k(x) = p^{a_2}x, \quad 0 \leqq a_\nu \leqq d \qquad (\nu = 1, 2) \tag{4.57}$$

where in the case of $a_\nu = d$ we can replace p^{a_ν} by 0. The order of $\mathfrak{A}/\mathfrak{K}$ is p^d, the order of $\mathfrak{A}^*/\mathfrak{K}$ is $p^n \geqq p^d$ so that the minimum condition on $\mathfrak{A}$ is satisfied.

In the case of $n = d$, $\mathfrak{A}$ and $\mathfrak{A}^*$ have equal orders and therefore they are both minimal. We can make an appropriate selection e. g. by requiring that A_0 should have a largest possible order. This leads to the supplementary conditions

$$n < d \quad \text{or} \quad n = d, \quad a_2 \geqq a_1 \tag{4.59}$$

which specify the canonical system (4.56), (4.57) uniquely.

Finally we consider invariants of the type (4.55). The corresponding canonical basis has the form

$$g_0(x) = p^{a_1+d_2} + qx, \quad 0 \leqq q < p^{d_2} \tag{4.60}$$
$$g_1(x) = p^{a_2}x, \quad g_2(x) = x^2$$

with

$$k(x) = b_1 p^{d_2} + b_2 x, \quad 0 \leqq b_\nu < p^{d_\nu} \qquad (\nu = 1, 2). \tag{4.61}$$

It can be shown that this system is equivalent to one with

$$q = p^{a_2}, \quad 0 \leqq a_2 \leqq d_2 \tag{4.62}$$
$$b_1 = p^{a_1}, \quad 0 \leqq a_1 \leqq d_1, \quad 0 \leqq b_2 < p^{a_2}.$$

The minimum condition on $\mathfrak{A}$ demands that $n + d_1 - a_1 \geqq d_1 + d_2$, i. e.

$$n \geqq a_1 + d_2 = a_1 + m. \tag{4.63}$$

If $n = a_1 + d_2$ then also $\mathfrak{A}^*$ is minimal and the invariants related to $\mathfrak{A}^*$ have the same form (4.60)—(4.62) as those related to $\mathfrak{A}$, with possibly different values of a_2, b_2. We can use either of the two systems to characterize this particular type of $\mathfrak{G}$.

5. In conclusion we set up a list of all "known" types of finite metabelian p-groups, that is classes of groups whose members have been determined explicitly. The catalogue does not contain every individual metabelian p-group which has ever been determined or described; a notable example of an exception is the maximal metabelian p-group with k generators and exponent p, determined by MEIER-WUNDERLI [4], which does not belong to either of these classes. But it should nevertheless give a fair idea of the extent to which the general structure problem of metabelian p-groups has been settled.

In the list below, $\mathfrak{A}$ denotes an abelian normal subgroup of the metabelian p-group $\mathfrak{G}$ with stated properties.

(1) $\mathfrak{G}$ of exponent p and generated by at most 5 elements.[10])
(2) $\mathfrak{G}/\mathfrak{N}$ of order p.[11])
(3) $\mathfrak{N}$ of exponent p, $\mathfrak{G}/\mathfrak{N}$ cyclic.[12])
(4) $\mathfrak{G}/\mathfrak{N}$ cyclic, $\mathfrak{G}$ generated by two elements.[13])
(5) $\mathfrak{N}$ of exponent p, $\mathfrak{G}/\mathfrak{N}$ abelian, $\mathfrak{G}$ generated by two elements.[13])

Numerous other metabelian group determinations of the past were omitted because they were included in at least one of the above classes. For example the classical Hölder case when both $\mathfrak{N}$ and $\mathfrak{G}/\mathfrak{N}$ are cyclic is included in (4).

Bibliography

. R. Brahana, Finite metabelian groups, *American Journal of Math.*, **62** (1940), 365—379.
[2] ——— Finite metabelian groups, *American Journal of Math.*, **73** (1951), 539—555.
[3] L. Kronecker and K. Hensel, *Vorlesungen über Zahlentheorie* (Leipzig, 1901).
[4] H. Meier-Wunderli, Metablesche Gruppen, *Commentarii Math. Helvetici*, **25** (1951), 1—10.
[5] L. Rédei, *Algebra I* (Budapest, 1954).
[6] ——— Äquivalenz der Sätze von Kronecker—Hensel und von Szekeres, *Acta Sci. Math.*, **17** (1956), 198—202.
[7] L. L. Scott, Finite metabelian groups, *Duke Math. Journal*, **20** (1953), 405—414.
[8] G. Szekeres, On a certain class of finite metabelian groups, *Annals of Math.*, **49** (1948), 43—52.
[9] ——— Determination of finite metabelian groups, *Transactions American Math. Society*, **66** (1949), 1—43.
[10] ——— A canonical basis for ideals, *American Math. Monthly*, **59** (1952), 379—386.

(Received March 17, 1960)

[10]) Brahana [1] and [2], also an extension to 6 generators by Scott [7], but the enumeration is not complete.
[11]) Determined in [9].
[12]) Determined in [8].
[13]) Determined in the present paper.